REMARKS

By the foregoing amendments, Applicants have deleted from claims 1 and 9 the restriction that the certificate-generation module is configured to prevent the computer from being controlled remotely. Although in most embodiments the certificate-generation module would likely be configured to verify that the messages it receives are in fact *bona fide* certification requests, it is the operating-system module that more typically will be most instrumental in guaranteeing that no external entity can mischievously access the certification authority's data or code. As mentioned below, Applicants have also amended claim 5 in response to the Examiner's § 112 rejection, and they have further revised claims 1-3, 5-7, 9, 14 and 15 to correct certain obvious inconsistencies and eliminate redundancies. Claims 1-16 are pending after the amendments.

35 U.S.C. §112

The Examiner rejected Claim 5 under 35 U.S.C. §112 as including the term *cert* without sufficient antecedent basis. Applicants have removed the basis for the rejection by replacing the term *cert* with the term *certification*.

35 U.S.C. §103

The Examiner rejected claims 1-16 under U.S.C. §103(a) as defining subject matter obvious in view of US Patent No. 6,490,367 to Carlsson and the cited webpage referred to in the office action as "Boot Disk Recovery." Applicants respectfully request that the Examiner reconsider this rejection, because Carlsson and Boot Disk Recovery do not

suggest a certificate-generation module contained on a bootable removable medium as Applicants' claims require.

By using Applicants' invention, an administrator can issue certificates from a plurality of locations. Now, it is true, as the Carlsson reference shows, that previous inventors had considered providing the administrator with multiple locations from which to issue certificates, but this was expensive if security was to be maintained. The conventional method of certificate generation requires devoting a machine exclusively to use as a certification-authority terminal, as Carlsson describes at column 3, lines 24-29. Physical security of the terminal must typically be maintained by isolating it in a protected room. Providing both security and multiple-location certificate issuance was therefore expensive.

Applicants recognized that they could provide flexibility, security, and efficiency by enabling an administrator to generate certificates without necessarily using a dedicated terminal. Their approach is to provide the certificate-generation software on a boot disk containing an operating system. Applicants do not claim to have invented the removable-boot-disk concept; that technology has a long history. But they were the first to use a boot disk containing both an operating system and a certificate-generation module. This approach enables an administrator to use almost any computer to generate certificates, and it maintains certification-authority security without wasting substantial resources.

Specifically, computers employed for general use require operating systems that provide a wide range of capabilities, including many communications capabilities. But providing such a wide range of capabilities results in vulnerabilities, such as vulnerability to remote operation, that are particularly problematic when the computer is configured to

operate as a certification authority. By using Applicants' invention, an administrator can employ a general-purpose computer for certification-authority purposes but limit such vulnerability to any desired extent. By booting the computer from a removable boot disk that contains an operating-system module with the certificate-generation module, that is, the administrator can bypass the computer's normal, full-featured operating system in favor of one whose capabilities are restricted enough to provide a desired degree of security. In particular, the removable-medium-resident operating system can be so configured as to prevent unwanted outside communication from infiltrating the machine. It can be configured, for instance, to allow only properly-formatted certification requests access to the certificate-generation module.

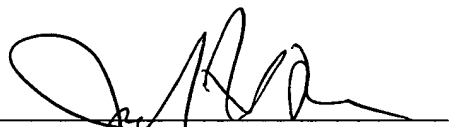
Applicants' method also frees resources because only a single removable medium needs to be physically secured; entire rooms do not have to be devoted to maintaining the certification authority's physical security. Since Applicants' method can be used with any computer that, as is typical, can be booted from the removable medium, the administrator is not restricted to using machines that he can afford to dedicate exclusively to use as a certification-authority terminal. So the administrator can generate certificates more conveniently. By using Applicants' method, the administrator can use human, machine, and building resources more efficiently.

The Examiner has rejected claims directed to this concept as defining subject matter obvious over Carlsson in light of the boot-disk concept that the "Boot Disk Recovery" reference describes. But boot disks had been known essentially from the dawn of the personal-computer age, yet practitioners in the certification-authority field have resorted to

the less-efficient prior-art methods. Had Applicants' method been obvious to workers in that art, they would have availed themselves of its advantages. That they did not demonstrates its unobviousness.

Applicants therefore request that the Examiner allow all claims.

Respectfully submitted,



Date: July 22, 2004
Customer No: 25181
Patent Group
Foley Hoag, LLP
155 Seaport Blvd.
Boston, MA 02210-2600

Joseph H. Born, Reg. No. 28,283
Attorney for Applicants
Tel. No. (617) 832-1134
Fax. No. (617) 832-7000